dsl2002.213.00

Project: Architecture & Transport Working Group

Title: Proposed Draft (PD)
DSL Evolution - Architecture Requirements for the Support of QoS-Enabled IP Services

Source:

BellSouth Inc.	**SBC Communications Inc.**	**Verizon Communications Inc.**
Tom Anschutz	Keith Allen	Michael Brusca
Al Blackburn	Mark Elias	Sanjay Udani
Ed Shrum	Will Chorley	
Barbara Stark	Doug Dean	
Albert Whited	Bart Hawkins	
	Mark Hubscher	
	Bill Hurst	
	Jeff Multach	
	Mike Sinwald	
	Tom Soon	
	Kuo-Hui Liu	
tom.anschutz@bellsouth.com	kxliu@tri.sbc.com	sanjay.k.udani@verizon.com

Date: August 20, 2002

Distribution: Architecture & Transport WG

Abstract:

At the May 2002 DSL Forum meeting, a formal call for contributions was made to develop a requirements document, given that a substantial number of contributions have been incorporated into WT-075, Network Migration. This contribution proposes that a Proposed Draft (PD) be created for Architecture Requirements for the Support of QoS-Enabled IP Services. In this contribution, a set of requirements is proposed along with a reference architecture. This builds upon other DSL Forum Technical Reports, such as TR-025.

DSL Forum

Proposed Draft

PD-00X

Revision 1.0

DSL Evolution - Architecture Requirements for the Support of QoS-Enabled IP Services

For
Architecture and Transport Working Group

August 2002

Abstract:
This Proposed Draft will outline an evolution of mass market DSL services to deliver multiple levels of QoS enabled IP layer services to DSL subscribers. In support of this service evolution, a reference architecture and supporting requirements are included that outline the interface specifications needed from a subscriber or a Service Provider to access these new services.

Table of Contents

Table of Figures

1 SCOPE AND PURPOSE

1.1 Scope

This document presents a proposal for evolving DSL deployment and interconnection. It outlines a common methodology for delivering QoS-enabled applications to DSL subscribers from one or more Service Providers.

1.2 Requirements

In this document, several words are used to signify the requirements of the specification. These words are often capitalized.

MUST	This word, or the adjective "REQUIRED", means that the definition is an absolute requirement of the specification
MUST NOT	This phrase means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications must be understood and carefully weighted before choosing a different course.
MAY	This word, or the adjective "OPTIONAL", means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option.

2 PRODUCTS AND SERVICES

2.1 Service Goals

DSL services have historically been bounded by the limitations specified when the service was first established. Subscribers placed orders for service based on a set speed profile purchased for a fixed amount of money recurring on a monthly basis. As newer features and services became available, the typical subscriber may or may not have been able to access these new services depending upon how their initial connection was established. Further, if the subscriber desired to modify their service to add more bandwidth, a new service profile had to be put into place. This service change was not a dynamic process. It took time to place, review, and process these orders and will involved some degree of service downtime before the subscriber was able to benefit from the increased bandwidth.

Despite efforts to unify the architecture of Service Provider connections and to provide common service tiers, there has not been general support for a unified architecture. This proposal intends to increase the interest in such an architecture by increasing the number of service parameters available as well as by making those parameters more dynamic. Aside from variable dynamic bandwidth, this new architecture includes Quality of Service (QoS) and multi-application/multi-destination selection.

Service Providers benefit in that they will only need to develop one set of system interfaces for any carrier that adopts this architecture. By subscribing to these interfaces, Service Providers will now be able to develop applications that can take advantage of variable bandwidth and better than "best effort" data traffic delivery. Subscribers will be able to realize greater potential of their broadband data connections. This means that a subscriber can still use their Internet access as it exists today; yet additional bandwidth on their DSL line can be used to deliver other applications, such as direct corporate access, video chat and video conferencing, and various content on demand, be it movies, games, software, or time-shifted television programs. Finally, these applications can be given QoS treatment, so that business access, online gaming, and casual Internet access all share bandwidth appropriately. Both subscribers and Service Providers will be able to decide among connections, who provides the best service for a specific application, and what applications add the most value.

2.2 Product and Service Definitions

This document presents a proposal for evolving DSL deployment and interconnection. It will outline a common methodology for delivering QoS-enabled applications to DSL subscribers from multiple Service Providers. These products and services are intended to address the mass market, and do not preclude additional niche or

custom services that could be provided using the same infrastructure. Many of the current products offered today either can be adapted to contain or already do contain the necessary software needed to support the proposed architectures contained within this document.

Also provided is a set of architectural requirements to support the proposed new service models. Some of the highlights including:

- IP-based services and QoS
- A single network control plane
- The migration of DSL to leverage newer, alternative transport technologies

With this target architecture in mind, a transition plan that identifies an interim phase before reaching the target is also included.

The prevalent existing service model, where subscriber connections are delivered in a best effort fashion over ATM PVCs, will continue to exist. However, this service model cannot support many of the improvements and benefits desired, including IP QoS, bandwidth on demand, and utilization of newer, alternative transport options.

Therefore, new service models for interconnection are put forward. Specifically, the following new and emerging service models are espoused and provide the benefits as listed:

Subscriber access using PPPoE aggregated into L2TP tunnels delivered to Network Service Providers. This access model is already being strongly adopted by many Service Providers. It can make good use of newer transport options (like Gigabit Ethernet), allows a Service Provider to continue to manage their own addresses and authentication, offers the ability to gain bandwidth on demand, and allows multiple simultaneous accesses by different subscribers to different Service Providers over the same access line.

Subscriber access using PPPoE or IP over Ethernet aggregated into VPNs delivered to Network Service Providers. As the ability to scale VPNs comes of age, this model offers all the benefits of the previous model, but also adds the ability to provide IP QoS on a packet-by-packet basis, and bandwidth on demand on a per-flow basis. This model also provides the opportunity for reduction in NSP capital expense and operational expense required to support either a layer 2 Network Server (LNS) or Broadband Remote Access Server (BRAS) in their networks.

Subscriber access using PPPoE or IP over Ethernet aggregated into a common, public, QoS-enabled IP network and delivered to Application Service Providers. A new service model is proposed to more efficiently manage scarce IP network address resources. For Service Providers that are more interested in providing their applications (like gaming, content, etc.) rather than a network infrastructure – there will be a common public DSL infrastructure on which addressing and network access mechanisms will be included. Application Service Providers will not manage IP addresses, nor authenticate subscriber access to the network, however, they will still authenticate user access to their applications in conventional ways.

In order to support these new products, the DSL service must be more than just a basic transport mechanism.

This DSL architecture and requirements put forward by this document enables these products and services. The following is a list of some of the new capabilities and features of these products.

- Bandwidth on Demand: The ability to dynamically change DSL line bandwidth based on the application or destination selected. This feature permits the subscriber to typically use a lower speed connection and occasionally request a dynamic increase in bandwidth based on application, Service Provider, or even a "Turbo" button.

- QoS/CoS on Demand: The ability to treat traffic dissimilarly to and from the subscriber based on specific usage characteristics of the product or service. This will permit high priority traffic to take precedence over other traffic destined for a specific subscriber. This may also be used to provide an optimized delivery through the Access Network.

- Many-to-Many Access: The ability for multiple users to access more than one Service Provider simultaneously. Additional destinations can be corporations or ASPs. As shown in Figure 2, this will permit the subscriber to maintain their current ISP relationship, yet allow users to have access to other applications that may not be available over their ISP connection.

- Content Distribution: The ability to support content storage (caching) and IP multicasting at the edge of the network to reduce backbone resource requirements. This will permit efficient use of network resources without overtaxing the Service Provider connections or the Core Network.

Network Service Providers will be able to benefit from the aggregation capabilities of these new DSL Access Networks. Specifically, the architecture will also permit:

- Traffic Aggregation: The end-to-end ATM PVC models, whether VPC or VCC, do not provide a scalable solution. L2TP and IP are used to provide better scalability and efficiency.

- Improved Transport: Currently most DSL transport is done over ATM connections. By offering other transport options, like Packet over SONET (POS) and Metro Ethernet, this architecture can provide better scalability, reduced overhead, and increased flexibility over ATM.

- Simpler Provisioning: Because they are not directly linked to provisioning transport, L2TP and IP delivery models can reduce the level of per subscriber provisioning.

- Differentiated Services: Up until now, almost all DSL transport has been best effort delivery at a fixed rate. This new IP based architecture will permit Service Providers to offer differentiated treatment for certain traffic.

- Increased Access: In previous architectures, Service Providers could only reach those subscribers with whom they had a direct relationship. These new architectures permit a subscriber to connect simultaneously to multiple Service Providers for a variety of services. Service Providers no longer need to be the sole provider to their subscribers.

- Standard Connections: Up until now, each access provider has had their own set of interfaces for Service Providers. This proposal defines common interfaces for NSPs and ASPs. This means that the Service Provider need only develop a single interface to get all of these features for many access providers. Also, subscriber connections will be similar among Access Providers, allowing common CPE to be more widely deployed.

Support for these new services will require a new set of network management interfaces. These interfaces will be used by both Service Providers and Subscribers. Service Providers will be able to examine the network and see how their subscribers are provisioned. NSPs will also be provided an interface to control and troubleshoot subscriber connections.

Subscribers will be provided mechanisms for requesting these new services and signaling specific needs.

These requirements will support services like:

- Multicast audio and video media applications
- Video on demand applications
- Voice services
- Interactive gaming
- Variable bandwidth, both on demand ("Turbo" button) and by application

3 FUNCTIONAL ASSUMPTIONS

3.1 Key Terminology

The following definitions apply for the purposes of this document:

Access Network	The Access Network encompasses the DSL modems at the customer premises and their connection to the Access Node at the central office or remote site.
Access Node	The Access Node contains the ATU-C, which terminates the DSL signal, and physically can be a DSLAM, Next Generation DLC (NG-DLC), or a Remote Access Multiplexer (RAM). A DSLAM hub can be used in a central office to aggregate traffic from multiple remote physical devices, and is considered logically to be a part of the Access Node. When the term "DSLAM" is used in this document, it is intended to very specifically refer to a DSLAM, and not the more generic Access Node. The Access Node provides aggregation capabilities between the Access Network and the Regional Network. It is the first point in the network where traffic on multiple DSL lines will be aggregated onto a single network.
Broadband Remote Access Server (BRAS)	The BRAS is the aggregation point for the subscriber traffic. It provides aggregation capabilities (e.g. IP, PPP, ATM) between the Regional/Access Network and the NSP or ASP. Beyond aggregation, it is also the injection point for policy management and IP QoS in the Regional/Access Networks.
Core Network	The center core of the Regional Network. The functions contained herein are primarily transport oriented with associated switching or routing capabilities enabling the proper distribution of the data traffic.
Downstream	The direction of transmission from the ATU-C (Access Node) to the ATU-R (modem).
Edge Network	The edge of the Regional Network. The Edge Network provides access to various layer 2 services and connects to the Regional Network core enabling the distribution of the data traffic between various edge devices.
Layer 2 Tunnel Switch (L2TS)	The L2TS provides a second layer of PPP aggregation beyond the L2TP Access Concentrator (LAC). PPP sessions are switched between L2TP tunnels and are further aggregated and delivered to the NSP.
Loop	A metallic pair of wires running from the customer's premises to the Access Node.
Many-to-Many Access Sessions	The ability for multiple individual users or subscribers, within a single premises, to simultaneously connect to multiple NSPs and ASPs.
Regional Network	The Regional Network interconnects between the Network Service Provider's network and the Access Network. A Regional Network for DSL connects to functional equipment at a central office such as an Access Node within an Access Network. The function of the Regional Network in this document goes beyond traditional transport, and may include aggregation, routing, and switching.
Regional/Access Network	The Regional and Access Networks.

Routing Gateway	A customer premises functional element that provides IP routing and QoS capabilities. It may be integrated into or be separate from the ATU-R.
Subscriber	The client that is purchasing the DSL circuit from the Service Provider and is receiving the billing.
Upstream	The direction of transmission from the ATU-R (modem) to the ATU-C (Access Node).
User	Typically, a member, employee or guest at the Subscriber's household or business using the DSL circuit capabilities.

3.2 Broadband Provider Reference Definitions

Generally, services over a DSL access-based broadband network will be provided and supported by a number of different operational organizations. These organizations may be part of one company or more than one company. Leaving commercial issues aside, it is necessary to have a clear idea of the roles of the different organizations and how the functionality of equipment, network management, and test equipment can support their ability to discharge their roles for the benefit of the end customers. In order to provide a baseline with which to contrast, this document provides a common architectural view of DSL architecture in Figure 1.

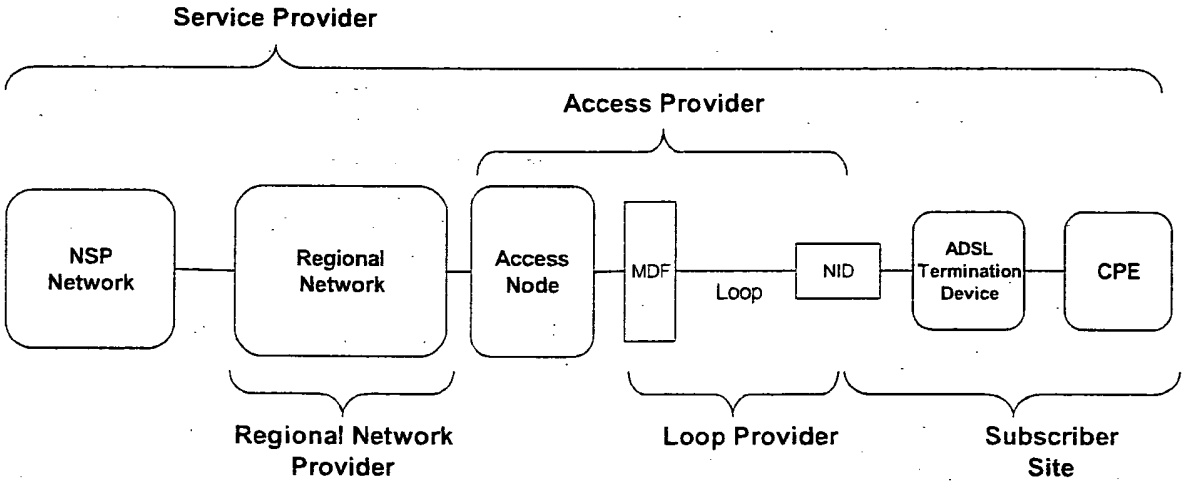

Figure 1 – DSL Network Components

(Voice components not shown for clarity)

Boxes in the figures represent functional entities – networks and logical components rather than physical elements.

This traditional architecture is centered on providing service to a line or a loop. It is desired, however, to be able to provide services that are user-specific. Additionally, more than one subscriber can be present at the same premises and share a single loop. There is a need, therefore, to describe a slightly more complex situation, and hiding the common complexity shared with Figure 1, this description is provided in Figure 2 below. Note that the figure shows many-to-many access through a common Regional/Access network. It is used to simultaneously provide an Application Service$_1$ between an ASP Network$_1$ and User$_1$ at the same time and over the same UNI as it supports a Network Service$_2$ between NSP Network$_2$ and User$_2$.

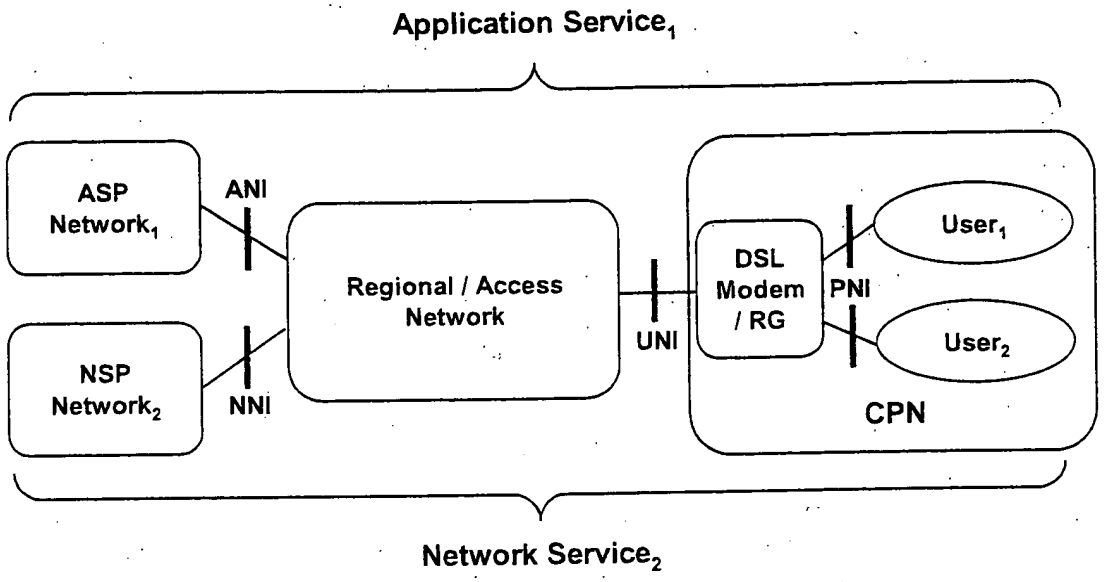

Figure 2 – Many-to-Many Access

The figures show the key components of a DSL access-based broadband network. They indicate ownership of the components to different providing organizations. The role of these various providers is indicated below:

The Network Service Provider (NSP):

- Includes Internet Service Providers (ISPs) and Corporate Service Providers (CSPs)
- Is responsible for overall service assurance
- May provide CPE, or software to run on customer-owned CPE, to support a given service
- Provides the customer contact point for any and all customer related problems related to the provision of this service
- Authenticates access and provides and manages the IP address to the subscribers

The Application Service Provider (ASP):

- Provides application services to the subscriber (gaming, video, content on demand, IP Telephony, etc.)
- Is responsible for the service assurance relating to this application service
- Responsible for providing to subscribers additional software or CPE which specific services may
- Provides the subscriber contact point for all subscriber problems related to the provision of specific service applications and any related subscriber software.
- Does not provide or manage the IP address to the subscribers

The Loop Provider:

- Provides a metallic loop from the Access Network equipment to the customer's premises
- Is responsible for the integrity of the metallic loop and its repair
- May also provide the Access Network Provider aggregated access to remotely deployed DSL equipment owned, operated, and maintained by the Loop Provider

The Access Network Provider:

- Provides digital connectivity to the customer via the metallic Loop
- Is responsible for the performance and repair of the access transmission equipment

The Regional Network Provider:

- Provides appropriate connectivity between the Access Network and the NSPs and ASPs
- Is responsible for Regional Network performance and repair

3.3 Interfaces

3.3.1 Application to Network Interface (ANI)

This reference point is between the Regional/Access Network and the ASP's Points of Presence (POPs). This interface will consist of a routed IP interface, that may be transported over Fast Ethernet, Gigabit Ethernet, Packet over SONET (POS), or some other IP interface. The ASP has the end-to-end Service responsibility to the customer for their specific application and is viewed as the "Retailer" of the specific service. Trouble reports for the specific service go directly to the ASP.

3.3.2 Network to Network Interface (NNI)

This reference point is between the Regional/Access Network and the NSP's POPs. The interfaces could be ATM, Fast Ethernet, Gigabit Ethernet, or Packet over SONET (POS). In the case of ATM, multiple sessions may be multiplexed over a single VCC at this interface. Typically, the NSP has the end-to-end service responsibility to the customer and is viewed as the "Retailer" of the service. As the retailer of the DSL service, trouble reports, and other issues from the subscriber are typically addressed to the NSP. Handoff protocols could include ATM VP/VCs, L2TP tunnels, and routed protocols using IP-VPNs.

3.3.3 User to Network Interface (UNI)

The User to Network Interface (UNI) is located at the subscriber premise between the Access Node and the Network DSL Termination Device. This reference point corresponds to earlier designations as the U Reference Point (as described in DSL Forum TR-043).

3.3.4 Premises to Network Interface (PNI)

The Premises to Network Interface (PNI) defines the interworking between the DSL modem/Routing Gateway and other CPE in the Customer Premises Network (CPN). The requirements for new vertical services over DSL require the addition of a Routing Gateway as the intermediate point between the DSL modem and the LAN Devices. The primary goal of this interface is to facilitate seamless transmission of IP packets in both a best effort approach as well as maintaining predefined QoS behavior or establishing dynamic QoS behaviors through a signaling mechanism. The DSL modem and Routing Gateway may or may not be a single device.

4 REFERENCE ARCHITECTURE

4.1 Logical Reference Architecture

As noted in Section 3.2 above, the end-to-end DSL network consists of four providers. Of these providers, the two that this proposal most affects are the Regional Network Provider and the Access Network Provider. Historically the Regional Network has been a network of ATM switches, as shown in Figure 3. This is because the access to most Access Nodes is an ATM based interface. Some Access Networks even have their own ATM switches used to aggregate traffic from multiple Access Nodes.

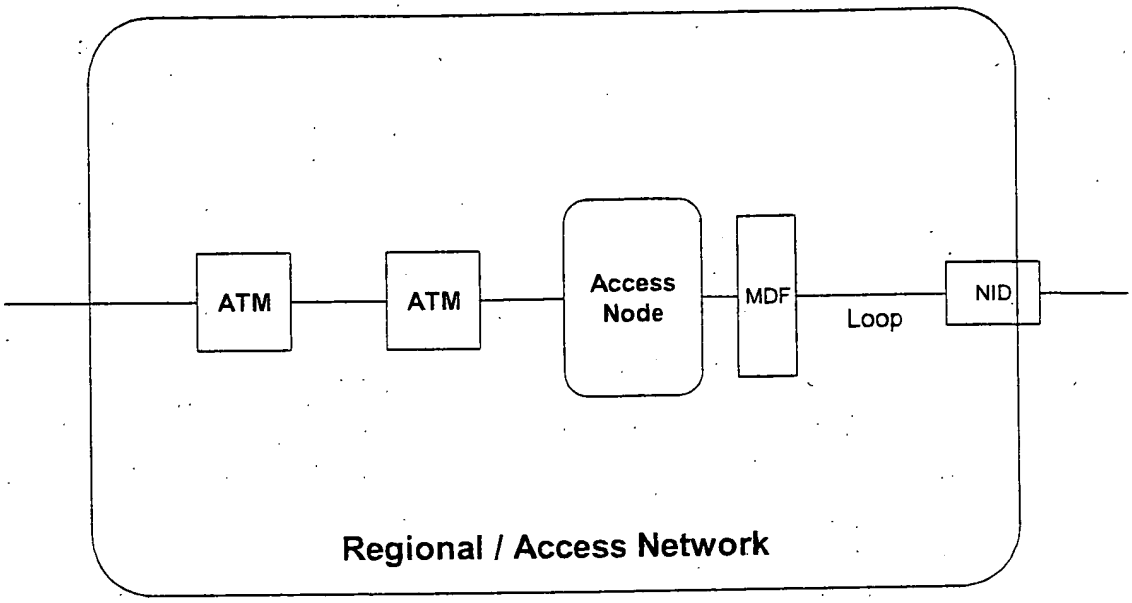

Figure 3 - ATM based Regional and Access Network Providers

In this architecture, there are no mechanisms for limiting subscriber traffic except for per line profiles within the Access Nodes. As many DSL networks were deployed before the advent of the BRAS, almost all the Access Network Providers use fixed speed profiles in the Access Nodes to limit upstream and downstream traffic. Even if the Service Provider were to attempt to send more traffic into the Regional Network than the Access Node is set to permit, the Access Node will police the downstream traffic. Since most Internet-based applications use TCP as the transport protocol, the traffic rejected at the Access Node will trigger TCP back-off, effectively throttling the downstream bandwidth. As such, most Service Providers also shape downstream traffic at the subscriber-selected bandwidth. However, the desire to move to a rate adaptive bandwidth model means that both the Regional and Access Networks could be vulnerable to traffic overloading. A means to control upstream and downstream traffic is needed as this architecture evolves.

Many times the physical components of the Access Nodes are daisy-chained, sharing the bandwidth of the aggregating circuit. As shown in Figure 12 in Section 4.2.5.4, there are numerous ways that DSL access devices can be interconnected to the first ATM switch. While historical measurements have shown that the typical DSL subscriber uses no more than a small fraction of sustained bandwidth, the fact is that as subscribers are offered more and more high bandwidth applications, the average sustained bandwidth per subscriber over these "mid-mile" connections is going to increase. As per subscriber bandwidth usage increases, the Regional Network Provider will also need to scale bandwidth and provide subscriber-level granularity. ATM VPs do not provide the granularity necessary to offer per application QoS on a per subscriber basis.

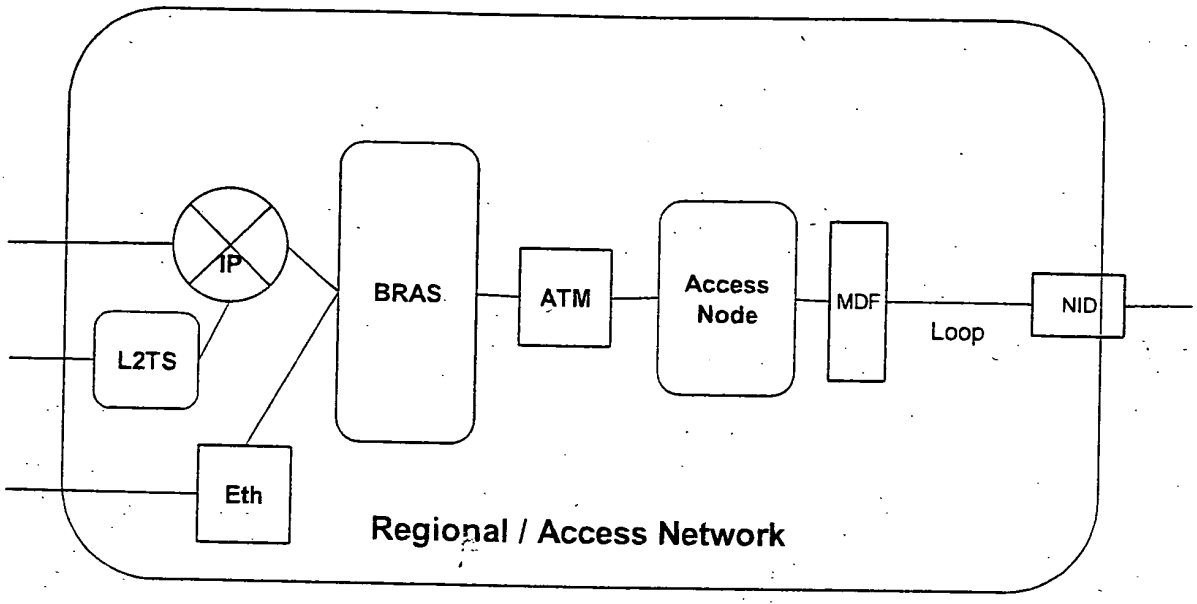

Figure 4 - IP Enabled Regional Network

As a result, other devices need to be added to the Regional Network to provide better aggregation of subscriber traffic. There are several options for doing this, most of which involve IP enabling the Regional Network as shown in Figure 4. Subscribers that use native IP, which is a routable protocol, can be aggregated at the IP level into a Virtual LAN (VLAN) or Virtual Private Network (VPN) for handoff to their associated Service Provider. Those subscribers that use variations of the Point to Point Protocol (PPP), such as PPPoA (PPP over ATM) and PPPoE (PPP over Ethernet), can be aggregated at either the PPP or the IP layer.

If the aggregation is done at the PPP layer, then these PPP sessions will need to be forwarded over a routable protocol such as Layer 2 Tunneling Protocol (L2TP). When the new subscriber aggregation element is functioning in this mode, it is referred to as an L2TP Access Concentrator or LAC. The other option for PPP based subscriber is to also terminate the PPP session and assign IP addresses to the subscribers. This traffic would then be collected into a VLAN or VPN as with native IP traffic. When performing PPP Termination and Aggregation (PTA), the box is typically called a Broadband Remote Access Server or BRAS.

As more and more DSL aggregation is performed at the IP layer rather than the ATM layer, additional transport options may be added. In addition to ATM, Ethernet and Packet over SONET are also options for IP transport. There are various metropolitan Ethernet solutions available in speeds of 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet), or 1 Gbps (Gigabit Ethernet or GigE). Metropolitan Ethernet connections have the added benefits of being less costly than Frame Relay, ATM, or private line circuits .

These new network elements also need to be able to function as the first tier ATM aggregation device, where the Access Node is now directly connected. As such, these devices will also need to handle ATM level aggregation and switching and need to function as an adjunct to the existing ATM network. Since they are IP aware, they can also serve as the Label Edge Router (LER) that is required if the Core Network is to become Multi Protocol Label Switching (MPLS) aware.

4.2 Logical Elements and Interfaces

4.2.1 Application Service Provider Network

4.2.1.1 Description

The Application Service Provider (ASP) is defined as a Service Provider that shares a common infrastructure provided by the Regional/Access Network and an IP address assigned and managed by the Regional Network Provider. This is a new application of DSL service. The Regional Network Provider owns and procures addresses that they, in turn, allocate to the subscribers. ASPs then use this common infrastructure in order to

provide application or network services to those subscribers. For example, an ASP may offer gaming, Video on Demand, or even filtered Internet access, or access to VPNs via IPsec or some other IP-tunneling method. The ASP service may be subscriber-specific, or communal when an address is shared using Network Address Port Translation (NAPT) throughout a Customer Premises Network (CPN). It is envisioned that the ASP environment will have user-level rather than network-access-level identification, and that a common Lightweight Directory Access Protocol (LDAP) directory will assist in providing user identification and preferences. Logical elements used by ASPs typically include routers, application servers, and directory servers. The relationship between the ASP Network, the ANI, and the Regional Network is shown in Figure 2.

4.2.1.2 Capabilities

The capabilities of the ASP include but are not limited to the following:

- Authenticating users at the CPN
- Assignment of user profile or preference data
- Assignment of QoS to service traffic
- Customer service and troubleshooting of network access and application-specific problems
- Ability to determine traffic usage for accounting purposes and billing

4.2.2 Application to Network Interface

4.2.2.1 Functionality

As shown in Figure 5, the Application to Network Interface defines the interworking between the ASP Network and the Regional/Access Network. This is not a traditional interface. However, in order to provide more technical and business options to would-be broadband content and application providers this document defines a way for a Service Provider to attach a server, servers, or entire network to a common infrastructure directly accessible by DSL subscribers. Providing the ANI is intended to promote content on demand, IP telephony, gaming, and other Quality of Service (QoS) or Bandwidth on Demand (BoD) applications without the need to deploy or manage an IP infrastructure. This also conserves IP addresses, as a single address can be used to gain access to all the services and providers that opt to share this infrastructure.

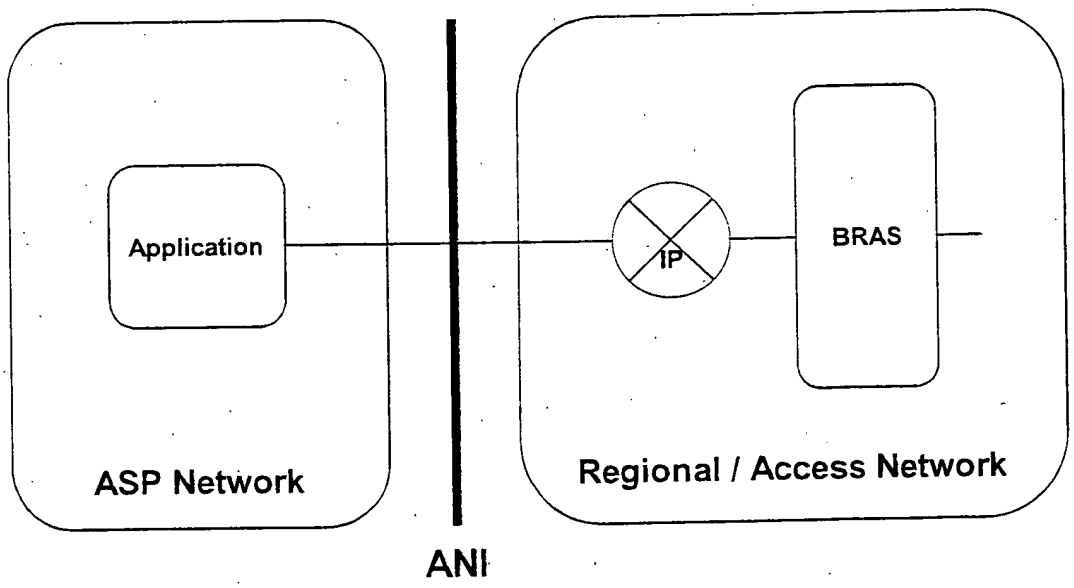

Figure 5 - Application to Network Interface

4.2.2.2 Communication Protocols

This interface MUST support IP networking connectivity to the DSL subscribers. Several QoS and BoD use cases exist:

1. Best effort IP networking is used with no additional QoS or information required.
2. Differentiated Services (Diffserv) QoS is provided in order to establish a higher class of service – oriented toward higher throughput, packet precedence, or lower latency.
3. RSVP-like (ReSource reserVation Protocol) signaling is used to receive bandwidth guarantees, BoD grants, or dynamic admittance to a strict priority Diffserv class.

The communications protocol stack is shown in the following Figure 6.

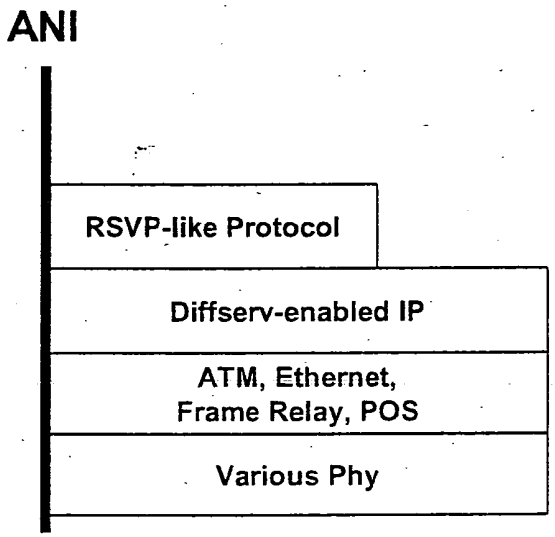

Figure 6 - ASP Protocol Stack with QoS

The ASP obtains an IP connection over a typical data link layer as described earlier. More likely is that an ASP actually obtains a 10 Base-T, 100 Base-T, or GigE connection to the Regional/Access Network within a co-location or hosting facility. The Regional/Access Network provider statically assigns the addresses, and MAY provide address blocks to the ASP.

Network Layer

The network layer interface MUST support IP version 4 in accordance with IETF RFC 1042.

The network layer interface SHOULD support IP multicast.

The network layer interface MAY support IP precedence based on Diffserv Code Point (DSCP) markings, in accordance with IETF RFC 3140.

The network layer interface MAY support IP precedence based on RSVP-like signaled QoS.

Data Link Layer

The data link layer SHOULD support Ethernet in hosting or co-location sites.

The data link layer MAY support ATM, Frame Relay, and/or POS.

Physical Layer

The physical layer interface MUST support the following:

- Ethernet PHY for 10 Mbps, 100 Mbps, 1 Gbps
- DS1, DS3

- OC3, OC12, OC48

4.2.3 Network Service Provider Network

4.2.3.1 Description

The Network Service Provider (NSP) is defined as a Service Provider that provides some service that requires extending a Service Provider-specific Internet Protocol (IP) address. This is the typical application of DSL service today. The NSP owns and procures addresses that they, in turn, allocate individually or in blocks to their subscribers. The subscribers are typically located in Customer Premises Networks (CPNs). The NSP service may be subscriber-specific, or communal when an address is shared using NAPT throughout a CPN. This relationship among the NSP, NNI, and Regional/Access Network is shown in Figure 2. NSPs typically provide access to the Internet, but may provide access to a walled garden, VPN, or some other closed group or controlled access services. L2TP and IP VPNs are typical NNI arrangements.

The capabilities of the NSP include but are not limited to the following:

- Authenticating network access between the CPN and the NSP network
- Assignment of network addresses and IP filters
- Assignment of traffic engineering parameters
- Customer service and troubleshooting of network access problems

4.2.4 Network to Network Interface

4.2.4.1 Functionality

As shown in Figure 7 and Figure 9, the Network to Network Interface defines the interworking between the NSP and the Regional/Access Network provider. This document offers the following Layer 2 and Layer 3 options for this interconnection.

4.2.4.2 Communication Protocols: L2TP Connection

This interface MUST support the Layer 2 PPP connection service supported by L2TP. Using Figure 8 as a reference, subscribers MUST be placed into L2TP tunnels in one of the following methods:

1. L2TP tunnels MAY be established or provisioned statically between LNS and the LAC or through an intervening Layer 2 Tunnel Switch (L2TS).
2. L2TP tunnels MAY be established dynamically using RADIUS in order to determine which users to add to various L2TP tunnels, including potentially new ones. As before, these may be directly between LAC and LNS or via L2TS.

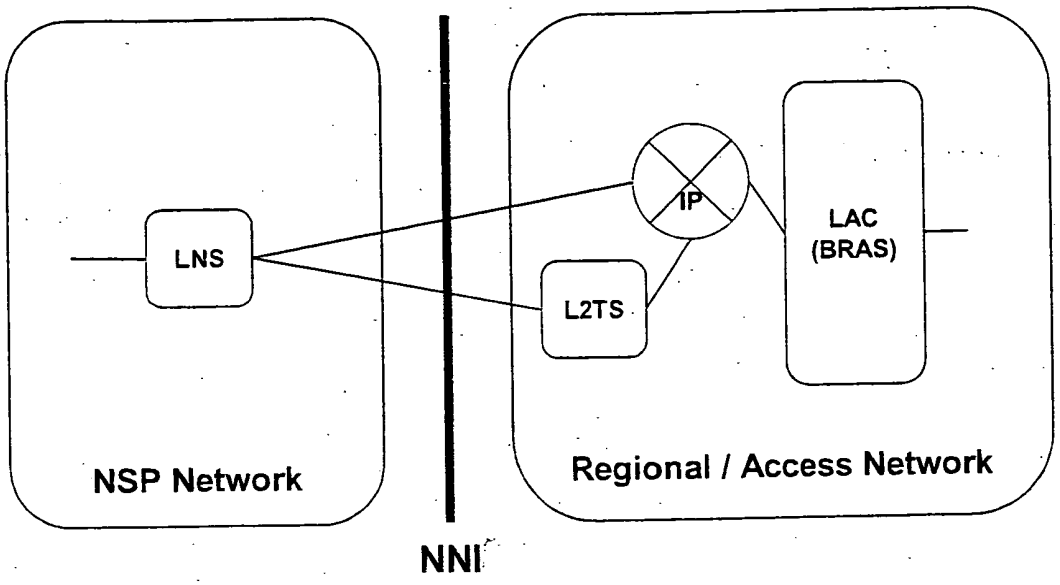

Figure 7 - Network to Network Interface supporting L2TP connection

One or more sessions can be established to NSPs and are chosen by the fully qualified domain name (FQDN) of the accessing subscriber.

Business models that require limiting subscriber access to a single NSP SHOULD be supported through administrative limits on the FQDN routing established by the Regional/Access Network provider on behalf of one or more NSPs. Subscribers SHOULD be able to establish multiple L2TP access sessions to the same or to different NSPs.

The RADIUS response MAY be used to determine the bandwidth profile for its access session.

The communications protocol stack is shown in the Figure 8.

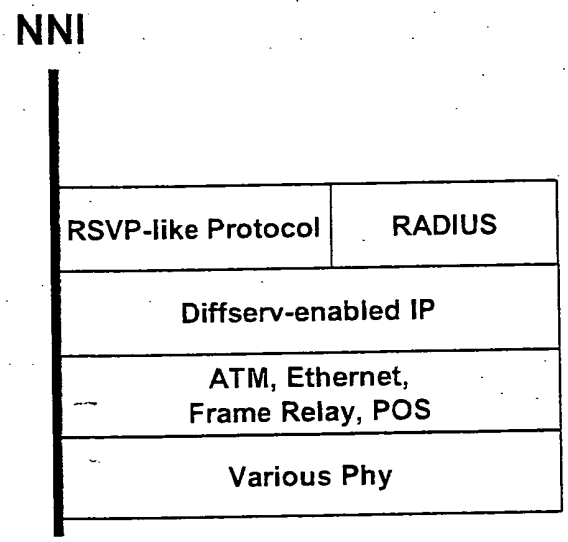

Figure 8 - L2TP Protocol Stack

While L2TP over IP MUST always be used, as opposed to L2TP delivered directly over ATM or Frame Relay, various IP transport options can be provided by the Regional/Access Network provider or selected by the NSP according to availability, regulation, and economics.

Network Layer

The network layer interface MUST support IP version 4 in accordance with IETF RFC 1042.

Data Link Layer

The data link layer SHOULD support ATM.

The data link layer MAY support Ethernet, Frame Relay, and/or POS.

Physical Layer

The physical layer interface MUST support the following:

- Ethernet PHY for 10 Mbps, 100 Mbps, 1 Gbps
- DS1, DS3
- OC3, OC12, OC48

4.2.4.3 Communication Protocols: IP Routed Connection

This interface MUST support the Layer 3 IP routed connection. Using Figure 9 as a reference, subscribers MUST be placed into IP routed networks in one of the following methods:

1. IP address pools MAY be established or provisioned statically.
2. IP addresses MAY be provided in pools that are distributed dynamically by the Regional/Access Network provider.
3. IP addresses MAY be established dynamically using RADIUS.
4. IP addresses MAY be assigned from named pools in cases where the NSP opts to allocate addresses out of two or more pools based on subscriber-specific information.

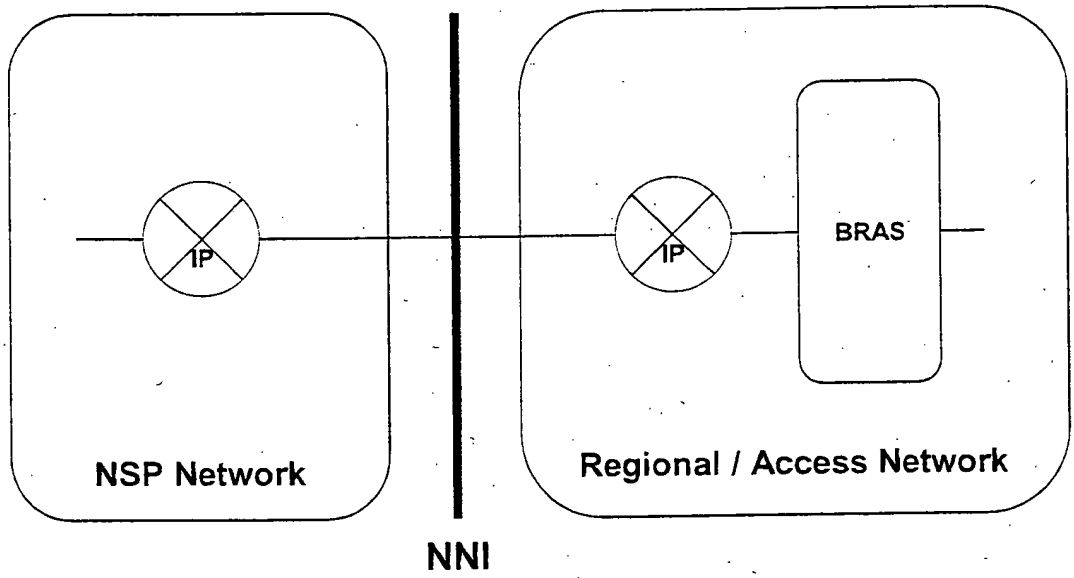

Figure 9 - Network to Network Interface supporting IP routed connection

In every case, RADIUS MUST be used between the BRAS (or a potential RADIUS proxy) and an NSP-designated AAA system or systems to authenticate subscriber access to the routed network.

In most cases, the IP routed network will be comprised of many IP-VPNs that support sharing of the Regional/Access Network at the IP layer.

Because multiple services are potentially provided across the UNI, access to the IP network will be governed, as with L2TP, using the FQDN of the accessing subscriber. Subscribers MUST be able to establish multiple

access sessions to the same or to different NSPs. Business models that require restricting the network access MUST be supported through administrative limits on the FQDN routing established by the Regional/Access Network provider on behalf of one or more NSPs.

If an NSP connects to the Regional/Access Network in several places, the NNI SHOULD support a dynamic routing protocol, like BGP, iBGP, or OSPF.

Several QoS and BoD use cases exist:

1. Best effort IP networking is used with no additional QoS or information required.
2. Diffserv QoS MAY be supported and MUST be used in order to establish a higher class of service – oriented either toward higher throughput, or lower latency.
3. RSVP-like signaling MAY be supported and MUST be used to receive bandwidth guarantees, BoD grants, or admittance to a strict priority Diffserv class.

The communications protocol stack is shown in Figure 10.

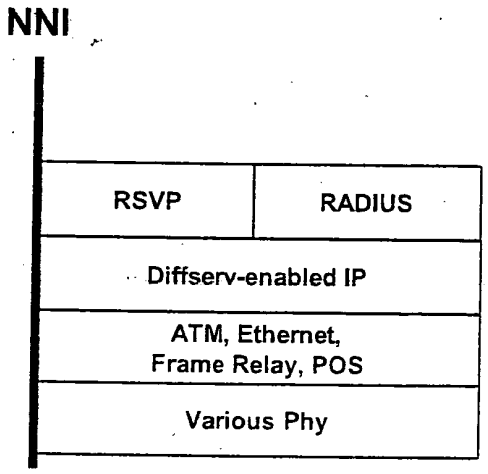

Figure 10 – Routed IP Protocol Stack with QoS

IP MUST always be used; however, various IP transport options can be provided by the Regional/Access Network provider or selected by the NSP according to availability, regulation and economics. As described earlier, RADIUS MUST always used to authenticate users, SHOULD be used to set NSP-desired filters, and MAY be used to assign addresses.

Network Layer

The network layer interface MUST support IP version 4 in accordance with IETF RFC 1042.

The network layer interface SHOULD support IP multicast.

The network layer interface MAY support IP precedence based on Diffserv Code Point (DSCP) markings, in accordance with IETF RFC 3140.

The network layer interface MAY support IP precedence based on RSVP-like signaled QoS.

Data Link Layer

The data link layer SHOULD support ATM

The data link layer MAY support Ethernet, Frame Relay, and/or POS.

Physical Layer

The physical layer interface MUST support the following:

- Ethernet PHY for 10 Mbps, 100 Mbps, 1 Gbps

- DS1, DS3
- OC3, OC12, OC48

4.2.5 Regional/Access Network

The Regional/Access Network consists of the Regional Network, Broadband Remote Access Server, and the Access Network as shown in Figure 11. Its primary function is to provide end-to-end transport between the customer premises and the NSP or ASP. The Regional/Access Network may also provide higher layer functions such as QoS and content distribution. QoS will be provided by tightly coupling traffic-engineering capabilities of the Regional Network with the capabilities of the BRAS. Depending on the type and frequency of use, certain content storage may be pushed further out in the Regional/Access Network than others. As a result, functionality to support content distribution could be located at different points within the Regional/Access Network, but will not be located between the BRAS and the subscriber.

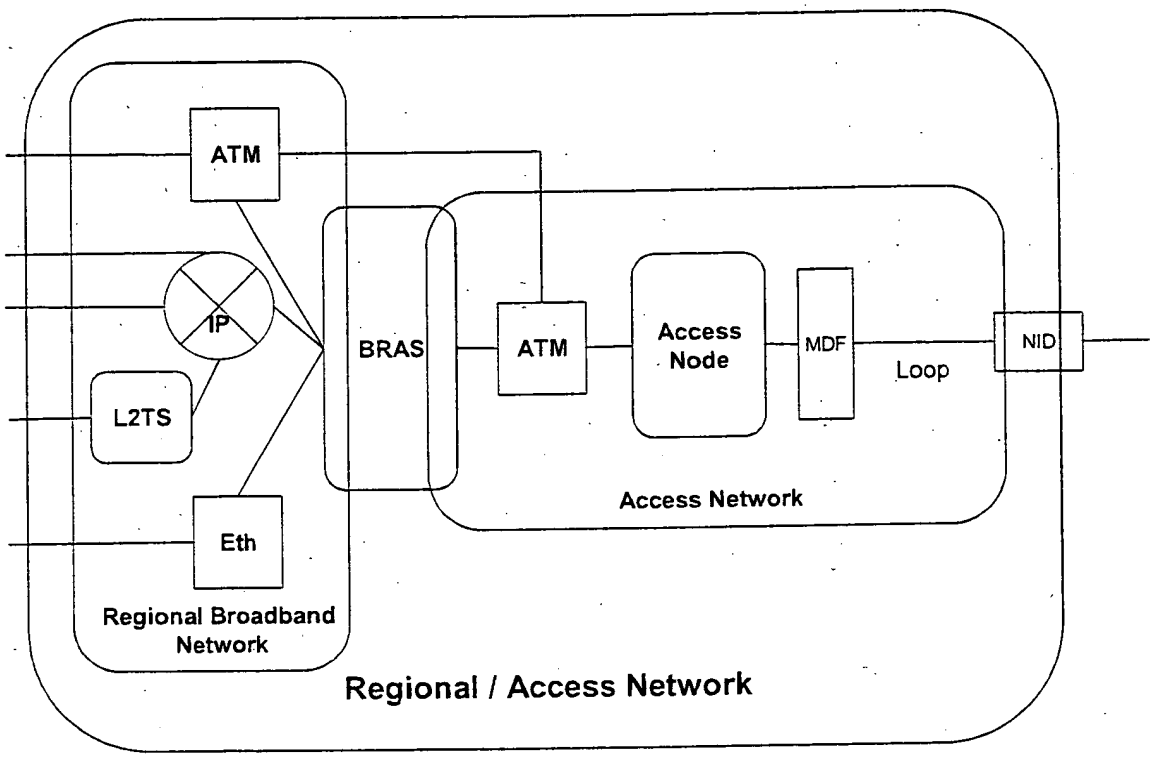

Figure 11 - Components of the Regional/Access Network

4.2.5.1 Regional Network

The Regional Network connects the BRAS and Access Network to NSPs and ASPs. The Regional Network may transport traffic using ATM, Ethernet, or IP MPLS. Within these networking technologies, the Regional Network MUST provide scalable traffic engineering capabilities to preserve IP QoS.

4.2.5.2 Broadband Remote Access Server

The BRAS performs multiple functions in the network. Its most basic function is to provide aggregation capabilities between the Regional/Access Network and the NSP/ASP. For the aggregation Internet traffic, the BRAS serves as a L2TP Access Concentrator (LAC) tunneling multiple subscriber PPP sessions directly to an NSP or switched through a L2TS. It also performs aggregation for terminated PPP sessions or routed IP session by placing them into IP VPNs or 802.1Q VLANs. The BRAS also supports ATM termination and aggregation functions.

Beyond aggregation, the BRAS is also the injection point for providing policy management and IP QoS in the Regional and Access Networks. The BRAS is fundamental to supporting the concept of many-to-many access sessions.

Policy information can be applied to terminated and non-terminated sessions. For example, a bandwidth policy may be applied to a subscriber whose PPP session is aggregated into an L2TP tunnel and is not terminated by the BRAS. However, sessions that terminate on (or are routed through) the BRAS can receive per flow treatment because the BRAS has IP level awareness of the session. In this model, not only can the aggregate bandwidth for a customer be controlled but also the bandwidth and treatment of traffic on a per application basis.

The delivery of content has shifted from content that was more download intensive with lower bandwidth and best effort quality to one that is more real-time in nature, requiring higher bandwidth with higher quality. Some of the higher bandwidth applications include Video on Demand (VoD) for movies, Multicast (Broadcast TV), and MPEG Unicast video. Given the BRAS's proximity to the edge of the network and its ability to support IP services, the BRAS MUST also provide support for content distribution and efficient use of multicast services.

Some high level functional requirements are for the BRAS are listed below. This list is not comprehensive and additional requirements for QoS are listed in Section 5.

- The BRAS MUST be able to aggregate PPP sessions in the L2TP tunnels.
- The BRAS MUST be able to switch PPP sessions between L2TP tunnels.
- The BRAS MUST be able to terminate PPPoE sessions and assign routing attributes based on subscriber profile.
- The BRAS MUST support authentication using RADIUS.
- The BRAS MUST support IP over bridged Ethernet (IETF RFC 2684).
- The BRAS MUST support address allocation using Dynamic Host Configuration Protocol (DHCP).
- The BRAS SHOULD support ATM VC/VP pass-through switching functions.
- The BRAS MUST support termination and aggregation of ATM VCs.
- The BRAS SHOULD support the following ATM classes of service: UBR, UBR+, CBR, VBR-nrt, VBR-rt .
- The BRAS MUST allocate downstream bandwidth based on policy configuration across ATM, PPP, Ethernet, and IP technologies.
- The BRAS MUST mark IP QoS fields for upstream and downstream traffic based on policy configuration.
- The BRAS MUST police IP QoS markings and bandwidth allocation based on policy configuration.
- The BRAS MUST support queuing and prioritization based on IP QoS marks.
- The BRAS MUST support traffic engineering for networking technologies including ATM, MPLS, and Ethernet.
- When operating in an IP-routed mode, the BRAS MUST provide multicast support by implementing:
  - Host Extensions for IP Multicasting defined in IETF RFC 1112
  - Internet Group Management Protocol, Version 2 (IGMP v2) defined in IETF RFC 2236
  - Protocol Independent Multicast-Sparse Mode as defined in IETF RFC 2362.
  - MBGP as per IETF RFC 2858
- The BRAS SHOULD support LAN interfaces for the local attachment of content distributions servers.

4.2.5.3 Access Network

Description

The Access Network refers to the network between the ATU-R and the ATU-C/Access Node. The protocols between these devices are well defined and this recommendation does not attempt to alter them.

4.2.5.4 Access Node

Description

The Access Node contains the ATU-C, which terminates the DSL signal. Physically, the ATU-C can be deployed in the central office in a DSLAM, or remotely in a remote DSLAM (RT-DSLAM), Next Generation Digital Loop Carrier (NG-DLC), or a Remote Access Multiplexer (RAM). A DSLAM hub can be used in a central office to aggregate traffic from multiple remote physical devices, and is considered logically to be a part of the Access Node.

The Access Node provides aggregation capabilities between the Access Network and the Regional Network. It is the first point in the network where traffic on multiple DSL lines will be aggregated onto a single network. Traditionally the Access Node has been primarily an ATM concentrator, mapping PVCs from the ATU-R to PVCs in the ATM core. The role of the Access Node will remain basically the same in the near term.

Various physical Access Node configurations are shown in Figure 12, with brief names for the configurations listed in Table 1.

The important aspect is that the daisy chaining never exceeds a depth of more than two ATM switching/multiplexing points in the Access Node.

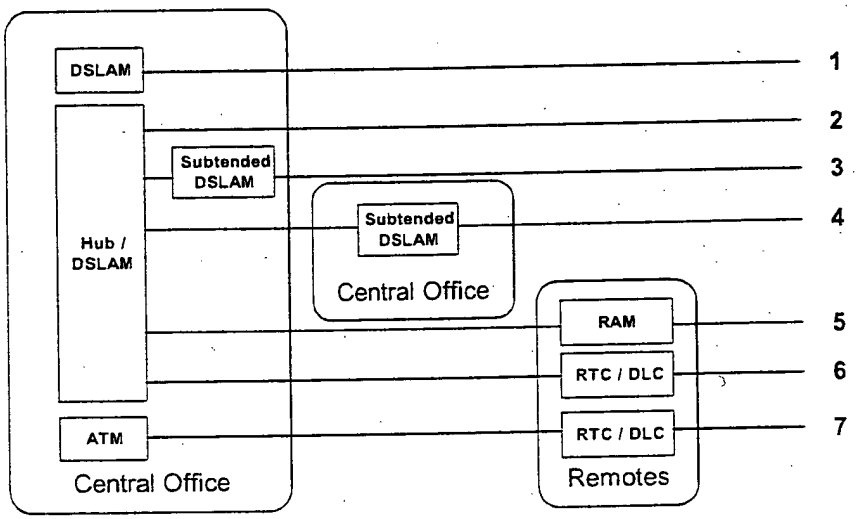

Figure 12 – Access Node Architecture Variations

Table 1 – Access Node Architecture Variation Descriptions

Reference #	Description
1	Access Node
2	Hub Access Node
3	Collocated Subtended Access Node
4	Remotely Located Subtended Access Node
5	Subtended Remote Access Node
6	Subtended DLC Located Access Node
7	Aggregated DLC Located Access Node

4.2.6 User to Network Interface

4.2.6.1 Functionality

The User to Network Interface (UNI) is defined as the interface between the Access Network and the CPN. This interface refers to the area between the CPN where the ATU-R (DSL Modem) is located and the Access

Network where the Access Node is located. The UNI includes the capabilities and protocols that cross between the Access Network and the CPN.

4.2.6.2 Communication Protocols

As shown in Figure 13 the User to Network Interface defines the interworking between the CPN and the Regional/Access Network. This interface MUST support the bi-directional delivery of data for all the new product and service definitions as well as for existing (legacy) products and services.

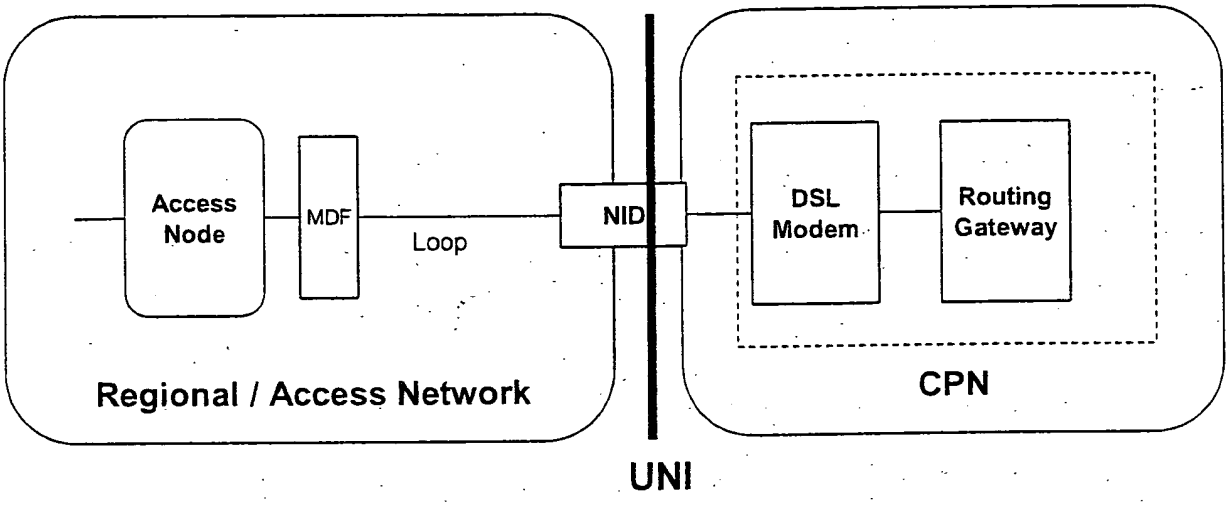

Figure 13 – User to Network Interface

Although the first Network Element connection in the network is at the Access Node, the User to Network Interface must support the transparent flow of protocols from the DSL Modem to the BRAS.

- The UNI MUST support at least one ATM AAL5 PVC per CPN using PPPoE and/or IP over Ethernet (IETF RFC 2684) configured using DHCP (for IP over Ethernet). A second ATM AAL5 PVC MAY be provisioned for real time applications.
- The UNI MUST support Diffserv Code Points (DSCP), enabling application-layer QoS signaling.
- The UNI MAY support signaled QoS, based on RSVP-like protocols.
- The UNI MUST support the ability to dynamically push IP routes back to the customer PC or Routing Gateway.

The communications protocol stack is shown in the following figure.

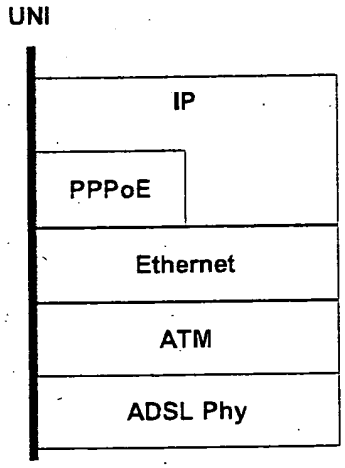

Figure 14 – UNI Protocol Stack

Network Layer

The network layer interface MUST support IP version 4 in accordance with IETF RFC 1042.

The network layer interface MAY support IP precedence based on Diffserv Code Point (DSCP) markings, in accordance with IETF RFC 3140.

The network layer interface MAY support IP precedence based on RSVP-like signaled QoS.

The network layer interface MUST support PPPoE per IETF RFC 2516.

Data Link Layer

The data link layer MUST support Ethernet encapsulation in accordance with IETF RFC 2684.

The data link layer MUST support ATM in accordance with ATM Forum standards.

Physical Layer

The physical layer interface MUST support G.dmt, and its related standards.

4.2.7 Customer Premises Network

The Customer Premises Network (CPN) is defined at its highest level as the location where the ATU-R is located and terminates the physical DSL signal, and where the subscriber's computers and other devices are interconnected.. The initial DSL deployments focused on single user architectures where the CPN constituted a single PC connected directly to a DSL modem. This paradigm of service will continue to be supported and improved, but must be extended to support advanced features that go beyond the single user model. To support enhanced features (multi-user, gaming, VoIP, video, etc), the CPN must evolve to support the networking and management of devices and services within the home or business location.

From a network perspective, the CPN is the ultimate target of the services provided by the Service Provider (NSP or ASP). The CPN includes the networking environment and protocols that are resident in the premises. A CPN may imply coexistence of different link and physical layer technologies such as radio, power line transmission and Ethernet, but is assumed to have access to outside networks (via DSL). The terms devices and appliances refer to the collection of end terminals that can reside on the CPN, either temporarily (laptops, palm pilots, foreign devices etc.) or permanently, such as desktops, security, and climate control systems. Devices may or may not be individually addressable and reachable from other devices, inside or outside the CPN. Some devices may communicate with proxies that then can relay or translate state or configuration information for these end devices.

4.2.7.1 DSL Modem

Description

The DSL Modem contains the ATU-R and terminates both DSL and ATM. It may or may not be integrated with additional Routing Gateway (RG) functionality. If it is not integrated, it will be used in a mode that is referred to as a simple bridge modem.

Capabilities

The capabilities of the DSL Modem MUST include but are not limited to the following:

- 2 ATM AAL5 PVCs
- UBR, UBR+ and VBR-rt ATM classes of service
- Per-VC queuing, separate priority queues for ATM classes of service

4.2.7.2 Routing Gateway

Description

CPN architectures typically leverage a Routing Gateway (RG) device that provides functionality beyond that of a basic DSL modem. The RG is a device for providing enhanced services within the CPN. The RG may or may

not be integrated with the DSL modem function. In the integrated scenario, the device terminates the DSL signal from the network and provides an interface to other equipment located within customer premises. In the non-integrated case, the RG is physically separate from the DSL modem and adds functionality to the CPN independent of the DSL modem. Since the integrated RG has knowledge of the CPN and its access to external networks, it enables tighter control of QoS for real time applications than may be possible in a non-integrated architecture. Both integrated and non-integrated RG are supported in this specification.

Capabilities

To support this QoS-enabled architecture, the capabilities of the RG MUST include but are not limited to the following:

- IP routing between the CPN and the Access Network
- Multi-user, multi-destination support: Multiple simultaneous PPPoE sessions (started from the RG or from devices inside the CPN) in conjunction with non-PPP encapsulated IP (bridged) sessions per IETF RFC 2684.
- Network Address Port Translation (NAPT)
- Local DHCP
- Support for major applications and protocols in the presence of NAPT and firewall (e.g., SIP, H.323, IPsec)
- Dynamic MTU negotiation
- Packet segmentation based on traffic/queue type
- PPPoE pass though
- Multiple queues, with the appropriate scheduling mechanism, e.g., Weighted Fair Queuing (WFQ).
- IP QoS
  - Classification and shaping of IP flows
  - Diffserv
  - Management interface
  - RSVP-like signaling
  - Support for real time services (Voice, Video)
  - Re-classification capabilities

4.2.7.3 Networking Technologies

Description

The CPN will support the transparent transmission of IP packets. It is expected that the CPN will be a hybrid of technologies that may include Ethernet, phone line networking, power line networking, wireless networking, and others.

4.2.7.4 LAN Devices

Description

Devices inside the CPN that are served by the DSL Modem and RG, and connected by the various Networking Technologies are referred to as LAN Devices. These may include, but are not limited to, PCs, laptops, networked set-top boxes, and Internet Appliances.

4.2.8 Premises to Network Interface

4.2.8.1 Functionality

As shown in Figure 15, the Premises to Network Interface (PNI) defines the interworking between the DSL modem/RG and the LAN Devices. This interface MUST support the bi-directional delivery of IP packets between the RG and other CPE as well as the ability to assign addresses to other CPE using DHCP. The other major functional requirement placed on the PNI includes identifying and supporting "QoS flows" as defined in Section 5. The primary goal of this interface is to facilitate seamless transmission of IP packets in both a best effort approach as well as maintaining predefined QoS behavior (Diffserv) or establishing dynamic QoS behaviors through a signaling mechanism (like RSVP).

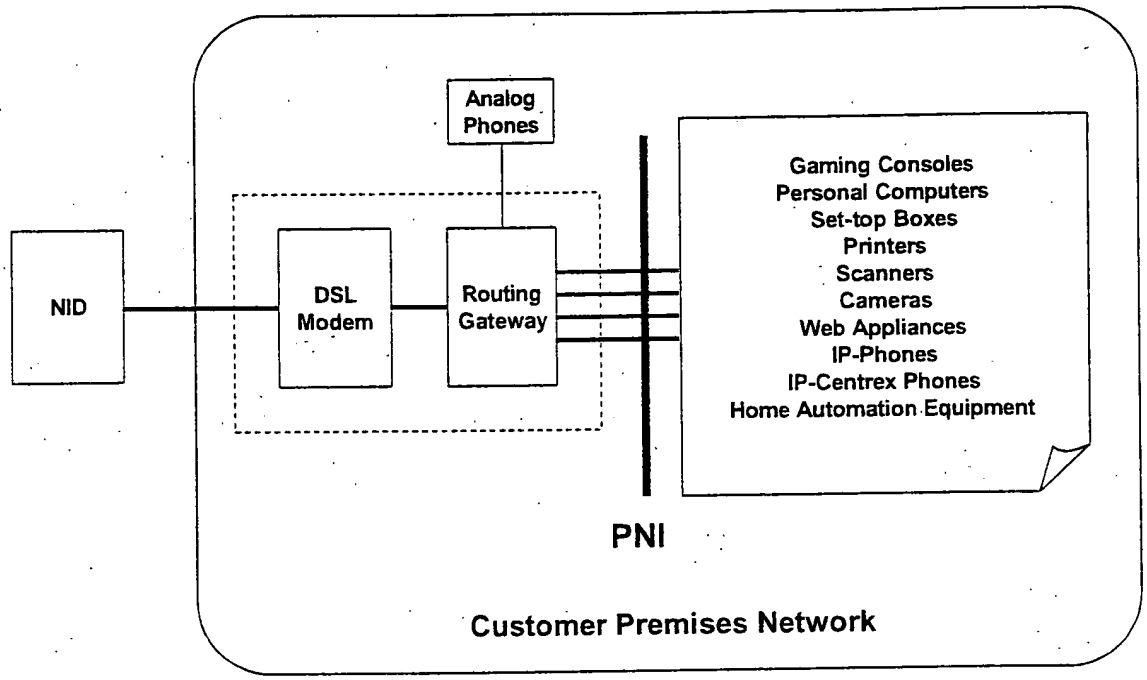

Figure 15 - Premises to Network Interface

4.2.8.2 Communication Protocols

Network Layer

The network layer interface MUST support IP version 4 in accordance with IETF RFC 1042.

The network layer interface MUST support IP precedence based on differentiated service (Diffserv) code points in accordance with IETF RFC 3140.

The network layer interface MUST support IP precedence based on RSVP-like signaled QoS.

Data Link Layer

The data link layer MUST support Ethernet in accordance with IEEE 802.2/802.3 (Ethernet) and as shown in Figure 16.

The data link layer SHOULD support Ethernet virtual LANs (IEEE 802.1Q).

The data link layer SHOULD support Ethernet precedence of LAN traffic (IEEE 802.1D/Q).

The data link layer MUST support PPP over Ethernet in accordance with IETF RFC 2516 and as shown in Figure 17

Logical Link Controller (LLC) Sublayer

The logical link controller sublayer subinterface MUST support Ethernet in accordance with IEEE 802.2.

Medium Access Control (MAC) Sublayer

The medium access control sublayer subinterface MUST support Ethernet in accordance with IEEE 802.3.

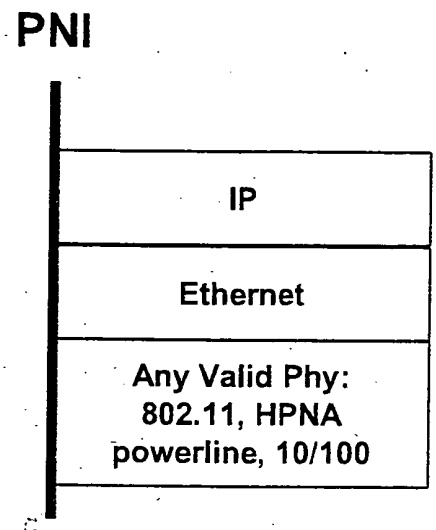

Figure 16 - IP over Ethernet

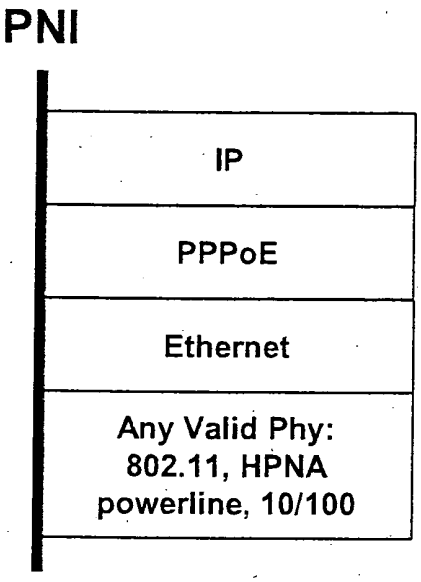

Figure 17 - IP over PPP over Ethernet

5 QUALITY OF SERVICE

5.1 Introduction

DSL architectures and products are predominately engineered for the support of best effort Internet traffic. Many NSPs desire the ability to improve their best effort product by using different levels of over subscription. Additionally, there are other market drivers pushing the Regional/Access Network to support differentiated services that require functionality beyond a best effort grade of service. Such services include telephony, video services, gaming, bandwidth on demand, and corporate VPN access as referenced in section 2.2. In order to support IP services effectively, the network must be IP aware and provide support that scales as the number of DSL subscribers and the number of applications per subscriber increases.

5.1.1 Goals

The goal of this section is to describe the mechanisms for introducing:

- A method for providing differentiated best effort traffic engineering
- Per flow IP QoS into the Regional/Access Network

Both of these goals leverage the existing capital investments yet effectively meet the goals for supporting differentiated non-real time and real-time IP applications.

One goal of the architecture is to enable more flexible bandwidth allocation to customers. It is a goal to allow both the customer and the various Service Providers to participate in defining the bandwidth that will be made available to them via DSL. This bandwidth can be provided at different rates not only at provisioning time or via service orders, but also on demand in near real time using mechanisms like "turbo buttons" at NSP or ASP web interfaces, or by using signaling protocols. It should be noted that this is still best effort bandwidth – there is no guarantee that an application can make use of the maximum bandwidth, in other words there are no throughput guarantees – only that the possible maximum rate might be increased.

Real-time applications have concerns beyond bandwidth, like jitter and latency, which become harder to manage when the DSL line rate slows down. Other applications, while may not be real time, have delivery requirements (no packets dropped) that cannot be assured by bandwidth alone. It is a goal to manage multiple applications over a small number (1 or 2) of ATM PVC(s) between the ATU-R and BRAS and provide the characteristics that both real-time and non-real time applications require.

5.1.2 Assumptions

Existing Regional Networks have a large embedded base of ATM equipment that is not IP aware. This equipment will be leveraged to the extent that it is technically and economically feasible.

5.2 Best Effort Traffic Engineering

Today's DSL access and Regional Networks are typically engineered to a single over subscription ratio picked by the various providers. This has served the market well, but may need to be enhanced as service diversity expands and scope broadens. The concept for best effort traffic engineering is that an NSP might be able to select an over subscription policy, and that the various NSPs can use that as a tool for providing different grades of service, even in an otherwise best effort model. Using this feature, one NSP may opt for highly over-subscribed infrastructure in order to provide an extremely cost-effective service, while a second NSP might choose a much less over subscribed approach in order to provide a better user experience or a premium service.

5.2.1 Theory of Operation

Best effort traffic engineering (TE) makes use of MPLS TE, ATM VP or VC, and L2TP features in order to provide a specific over subscription rate for that NSP.

As shown in Figure 18, traffic flowing between NSP_1 and CPN_1 is shaped to a large asymmetric configuration through the Regional/Access Network. At the same time, traffic flowing between NSP_2 and CPN_2 is shaped to a smaller symmetric configuration.. Finally, ATM or Diffserv techniques can be used at the NNI in order to divide the total bandwidth at the NNI among potentially disparate tunnel types that traverse it.

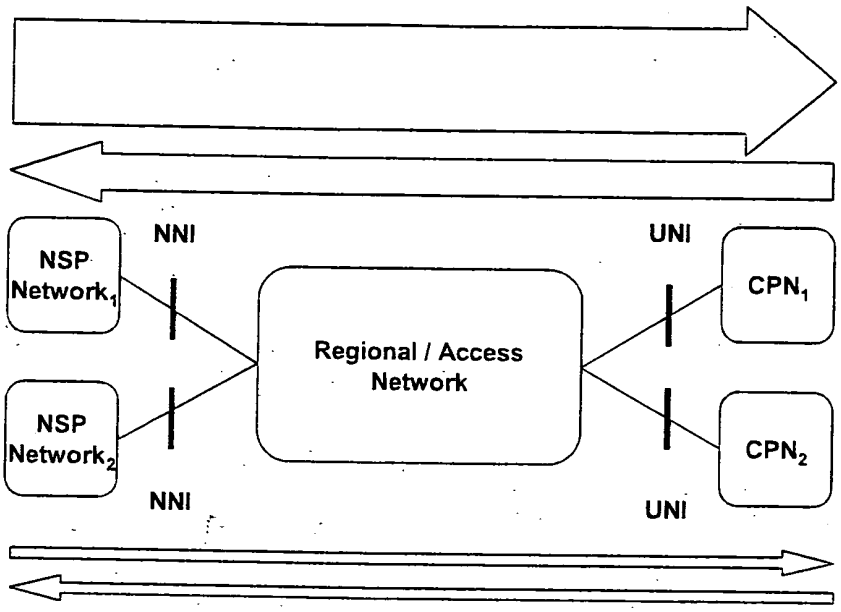

Figure 18 – Best Effort TE

5.3 QoS Architecture - A two-phase approach

While a signaled per flow IP QoS mechanism is the ultimate goal of this architecture, the technical and economic feasibility of such a build out can not be justified in the near term. Instead, a 2-phase approach is suggested that leverages incremental IP awareness associated with ATM level traffic engineering. In the first phase, IP aware network elements are added to the network that in conjunction with ATM traffic engineering can manage IP flows through non-IP aware devices. The Diffserv model is leveraged to prioritize and shape traffic through ATM devices. The bandwidth that a subscriber receives will no longer be determined by the DSL synch rate alone. Instead, both the physical and IP layers will be leveraged. Most importantly, phase 1 significantly increases the IP layer functionality of the Regional/Access Network while not requiring massive re-deployment of capital and re-engineering of the network.

Phase 2, however, will require more enhancements to the Regional/Access Network by eliminating or enhancing some ATM elements/functions and further increasing the IP capabilities. IP signaled QoS is introduced in this phase.

5.3.1 Phase 1 QoS Mechanisms

Phase 1 largely leverages the existing broadband Regional/Access Network as shown in Figure 3. This network is generally IP unaware. In order to efficiently add IP awareness to the network, two enhancements are required: Within the network the BRAS is leveraged to provide IP aware handling of traffic and, similarly, at the customer premises new CPE capabilities are deployed.

When a subscriber purchases a differentiated service, this service MUST flow through the BRAS. To support differentiated services, the BRAS preserves IP QoS through the access node and to the customer premises by shaping traffic based on the physical topology of the logical connection between the BRAS and the RG. In order to accomplish this task, the BRAS MUST be able to perform packet classification and hierarchical shaping and scheduling.

- The BRAS MUST support packet classification and scheduling in accordance with Diffserv.

- The BRAS MUST support hierarchical shaping and scheduling for the control of traffic through the access node and any other intervening devices that do not have IP awareness.

The effectiveness of using hierarchical shaping across non-IP aware devices decreases as the number of devices and the amount of non-BRAS controlled traffic increases. As a result, the BRAS function should be located as close to the access node as possible from an ATM hop perspective. The BRAS function MAY be integrated into the access node.

In order to preserve an IP flow's characteristics, the customer CPE must be involved in the QoS architecture. This is especially true when dealing with traffic destined for the upstream DSL connection. This connection is typically the slowest link and most likely to incur congestion and add delay and jitter within the service. To maintain fair but effective through put over this link the RG MUST support packet classification and scheduling in accordance with Diffserv. The RG MUST support fragmentation based on queue status and type.

The typical DSL customer is connected to the Regional/Access Network via a single ATM AAL5 PVC. This single PVC should be leveraged to the extent possible using the capabilities described above. Some applications or network topologies may require a more stringent level of QoS between the BRAS and the customer premises. A second ATM AAL5 PVC MAY be provisioned for services that require extremely tight delay/jitter tolerances. The number of PVCs per customer SHOULD NOT exceed 2.

To support bandwidth on demand products or other differentiated services that implicitly require additional bandwidth on demand, a subscriber's access sessions SHOULD be shaped and policed by the BRAS and RG instead of solely by the DSL ATU-R and ATU-C. This change is accompanied by changing the ATUs to allow them to synchronize at or near their maximum rate. Since we allow for multiple simultaneous access sessions, it MUST be possible to modify the shapers and policers on one or more sessions at the same time. The policy data for the classification and shaping of traffic at the RG is provided at service configuration and is not a real time capability. The policy data for the classification and shaping of traffic at the BRAS can be provided at service configuration or may be dynamically configured via a Common Open Policy Service-like (COPS) interface.

5.3.1.1 Diffserv Requirements

RG

The RG requirements below only apply to the support of differentiated services.

The RG MUST be the central point for controlling traffic within the customer premises and traffic destined for the Access Network.

The RG MUST support Diffserv marking and reclassification in accordance with IETF RFC 2474.

The RG MUST support Diffserv queuing for the Assured Forwarding (AF) and Expedited Forwarding (EF) classes in accordance with IETF RFC 2597 and IETF RFC 3246 for carrying real time traffic. The exact AF classes supported will be described in future revisions to this document.

The RG MUST support multiple queues with the appropriate scheduling mechanism to effectively implement Diffserv queuing behaviors (e.g. strict priority, Weighted Fair Queuing).

The RG MUST be configured with the classification parameters for mapping traffic into a given Diffserv Per Hop Behavior (PHB) during service configuration.

The RG MUST support fragmenting large data packets in the Best Effort (BE) and AF queues when packets are present in the EF queue.

The RG MUST support an EF window timer. The EF window timer is required to support real time applications that exhibit a more bursty nature (e.g. VoIP with silence suppression) so that BE and AF packets continue to be fragmented even when EF packets are not present.

When no packets are queued in the EF class for a duration longer that the EF window timer, the BE and AF packets MUST NOT be fragmented unless required for other reasons (negotiated MTU size).

If multiple PVCs are present, the RG MUST support the mapping between a Diffserv Code Point (DSCP) and a specific PVC.

BRAS

The BRAS MUST support Diffserv marking and reclassification in accordance with IETF RFC 2474.

The BRAS MUST be able to police the use of DSCPs received from customer traffic and remark traffic as BE if it does not match the customer profile data.

The BRAS MUST support Diffserv queuing for the Assured Forwarding (AF) and Expedited Forwarding (EF) classes in accordance with IETF RFC 2597 and IETF RFC 3246. The exact AF classes supported will be described in future revisions to this document. These queues are defined within the context of the DSLAM connectivity between the BRAS and the access node in affect managing the access node's downstream bandwidth.

The BRAS MUST support multiple queues per user with the appropriate scheduling mechanism to effectively implement Diffserv queuing behaviors (e.g. strict priority, Weighted Fair Queuing).

The BRAS MUST support the mapping of DSCP to MPLS LSP, VLAN, ATM VP, or other traffic engineering capabilities in the Regional Network.

5.3.1.2 Traffic Engineering Requirements

In order for the BRAS to effectively manage IP traffic through layer 2 devices, the BRAS MUST have awareness of the all of the traffic that is traversing those layer 2 elements. This can be accomplished to 2 ways. The first and most straightforward method is for all traffic destine for the access node to flow through the BRAS enabling it to shape the traffic accordingly. In cases where this is not possible, then the amount of aggregate resources that is not under the control of the BRAS must be subtracted from the resources that the BRAS has under its control and be factored into the shaping and scheduling functions. The traffic that is not under the control of the BRAS MUST be traffic engineered in a way that it cannot consume resources above the amount that the BRAS is aware of.

5.3.1.3 Admission Control

Network level admission control is not required in this phase. Admission control MAY be provided at the application layer. That is, the application can restrict the number of active sessions per access node and per customer premises.

5.3.2 Phase 2 QoS Mechanisms

The architecture for the second phase of the QoS enhancements is not fully defined in the following section. This section is included for illustrative purposes and will be fully defined in future documents.

Phase 2 adds per IP flow resource reservation capabilities in the Regional/Access Network. Phase 2 continues to leverage the BRAS as the IP QoS manager of the access node. Rather than simply managing the aggregate scheduling of Diffserv resources, the BRAS will be able to perform per flow admission control ensuring that resources are never over booked. Diffserv will continue to be used beyond the BRAS for scalability reasons. Keeping per flow resource reservation limited to the access portion of the Regional/Access Network will limit scalability/performance issues known with prior end-to-end reservation schemes.

5.3.2.1 Signaled QoS Requirements

BRAS

The BRAS MUST support a RSVP-like protocol for the assignment of resources. When resources are not available at any point under its control the BRAS MUST block the admission of the session and provide feedback to the initiating host.

The BRAS MUST know the DSL synch rates of the ATU-Rs that are connected to the access nodes that it manages. Based on a given ATU-R's DSL synch rate and customer profile the BRAS must manage the admission of sessions to that customer premises. An external policy/management server MAY feed this information to the BRAS.

The BRAS MUST be able to intercept RSVP and application layer (e.g. SIP) messages that are not addressed to it and use these messages in making admission decisions.

The BRAS MUST support mapping reservation requests into Diffserv PHBs and managing the PHBs as reservable resources.

CPE

The CPE requirements below only apply to the support of differentiated services.

The CPE requesting differentiated services MAY be integrated with the ATU-R. Non-integrated CPE devices will also be supported (e.g. IP Phones, PC running video conferencing software, set top boxes, etc).

The CPE MUST support IP layer signaled QoS similar to the IETF RSVP specification. These messages MUST be addressed to the destination host and MUST NOT be addressed directly to the BRAS.

The CPE MUST NOT make any admission decisions.

5.3.2.2 Diffserv Requirements

BRAS

The BRAS MUST conform to the requirements listed in section 5.3.1.1

The BRAS MAY accept policy information regarding how to manage Diffserv resources from an external entity.

CPE

The CPE MUST conform to the requirements listed in Section 5.3.1.1

If the signaling messages indicate the DSCP to be used by a session requesting access, the CPE MUST use the specified DSCP.

The CPE MAY accept policy information regarding how to manage Diffserv resources from an external entity.

5.3.2.3 Traffic Engineering Requirements

The RSVP-like mechanism described only has resource knowledge of the local access node and does not have an end-to-end picture of the connection. As a result, the interconnection network within the Regional/Access Network (beyond the BRAS) MUST support traffic engineered to provide support for enhanced services. It is expected that within the core of the Regional/Access Network that aggregate traffic engineering techniques can efficiently serve the needs of enhanced applications.

The Regional/Access Network MAY support MPLS TE.

The Regional/Access Network MAY support ATM level TE.

The Regional/Access Network MAY support Diffserv.

5.3.2.4 Admission Control

Per-flow admission control MAY be performed at the BRAS. Admission decisions are made based on resource availability AND subscriber profile data. Both of these parameters may be sent to the BRAS via an external policy/provisioning server.

Application level admission control MAY be applied in addition to the network based admission control.

6 SERVICE LEVEL MANAGEMENT

6.1 Introduction

Service Level Management is intended to provide 3 levels of benefit – increasing over time:

- To provide a list of the salient network performance and operational metrics that might be used in a Service Level Objective (SLO) or Service Level Agreement (SLA).
- To provide a standard definition of such metrics so that its meaning would be common when used by various providers.
- To provide extreme values that are driven by architectural considerations where applicable. For example, while it is NOT the intention of this document to set the SLO or SLA for Network Delay (Latency), any

network that purports to support Voice over IP (VoIP) will need to have a maximum delay that is within the bounds necessary to support VoIP.

6.2 Network Performance Metrics

1. **Network Availability** - The percent of time that the Regional/Access Network is available for subscribers to connect. This metric is defined on some time basis, such as a month, a week, or a year. An SLA should also specify not the entire network but the section of the network for which the Regional/Access Network Provider is responsible. For example, the Regional/Access Network Provider is not responsible for NSP problems.
2. **Network Delay (Latency)** – The time it takes for a data packet to traverse the Regional/Access Network, from end-to-end or edge-to-edge. Latency is defined in milliseconds and can be a one-way or round-trip delay.
3. **Message Delivery** - The ability of the Regional/Access Network to transmit traffic at the negotiated speed. Some applicable measurements are packet loss). These metrics must have a time base as well.
4. **Network Jitter** – The variance of network latency. Jitter is defined in milliseconds.

6.3 Operational Metrics

1. **Mean Response Time** - The time it takes the Regional/Access Network Provider to respond to submitted reports of trouble
2. **Mean Time to Restore Service** – The measurement of the Regional/Access Network Provider's ability to restore service within the negotiated interval
3. **Ordering System Reliability** – The measurement of the consistent availability of ordering system.
4. **End-User Installation Guarantee** – The measurement of the Regional/Access Network Provider's ability to meet negotiated order due dates.

7 SERVICE MANAGEMENT

The architecture proposed in this document clearly needs management systems to provide the controls necessary to support the underlying service "building blocks". The following lists are examples of new data points that management systems MUST support. Network elements and Service Providers will use these new data elements for service provisioning and data delivery. It is expected that the Operations and Network Management working group of the DSL Forum will provide contributions to augment this section.

7.1 Subscribers

Because of the changes in how DSL is provisioned and managed, there are a number of new data points that must be tracked for each subscriber. Among these are:

- Maximum sustainable subscriber bandwidth
- Maximum number of sessions allowed
- Permitted destinations
- Default protocol
- Default destination
- Default bandwidth
- Single host or subnet needed
- Restricted subscriber (single destination only)
- Total reserved bandwidth

7.2 Service Providers

Because of the changes in how DSL is provisioned and managed, there are more details needed per Service Provider. When various choices listed for an option, these are to be considered as examples only and not a definitive list of the choices for a given option.

- Minimum bandwidth needed
- Minimum QoS level
- Various protocol metrics
- Subscriber protocol (IP, PPPoE)
- Protocol (IP, L2TP, ATM)
- Authentication
- IP address assignment
- Transport
- Maximum simultaneous sessions

APPENDIX A REFERENCES

[1] DSL Forum TR-010, "Requirements & Reference Models for ADSL Access Networks: The "SNAG" Document"

[2] DSL Forum TR-025, "Core Network Architecture for Access to Legacy Data Networks over ADSL"

[3] DSL Forum TR-032, "CPE Architecture Recommendations for Access to Legacy Data Networks"

[4] DSL Forum TR-037, "Auto-Configuration for the Connection Between the DSL Broadband Network Termination (B-NT) and the Network using ATM"

[5] DSL Forum TR-042, "ATM Transport over ADSL Recommendation (Update to TR-017)"

[6] DSL Forum TR-043, "Protocols at the U Interface for Accessing Data Networks using ATM/DSL"

[7] M. Kaycee, G. Gross, A. Lin, A. Malis, J. Stephens, "PPP over AAL5," IETF RFC 2364, July 1998

[8] L. Mamakos, et al, "A Method for Transmitting PPP Over Ethernet", IETF RFC 2516, February 1999

[9] D. Grossman, J. Heinanen, "Multiprotocol Encapsulation over ATM Adaptation Layer 5", IETF RFC 2684, September 1999

[10] W. Townsley, et al, "Layer Two Tunnelling Protocol (L2TP)" IETF RFC 2661, August 1999

[11] J. Postel, J.K. Reynolds, "Standard for the transmission of IP datagrams over IEEE 802 networks", IETF RFC 1042, February 01, 1988.

[12] S.E. Deering, "Host extensions for IP multicasting", IETF RFC 1112, August 01, 1989.

[13] W. Fenner, "Internet Group Management Protocol, Version 2", IETF RFC 2236, November 1997.

[14] T. Bates, Y. Rekhter, R. Chandra, D. Katz, "Multiprotocol Extensions for BGP-4", IETF RFC 2858, June 2000.

[15] K. Nichols, S. Blake, F. Baker, D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", IETF RFC 2474, December 1998.

[16] J. Heinanen, F. Baker, W. Weiss, J. Wroclawski., "Assured Forwarding PHB Group", IETF RFC 2597, June 1999.

[17] D. Black, S. Brim, B. Carpenter, F. Le Faucheur, "Per Hop Behavior Identification Codes", IETF RFC 3140, June 2001.

[18] B. Davie, A. Charny, J.C.R. Bennet, K. Benson, J.Y. Le Boudec, W. Courtney, S. Davari, V. Firoiu, D. Stiliadis, "An Expedited Forwarding PHB (Per-Hop Behavior)", IETF RFC 3246, March 2002.

[19] The ATM Forum "Traffic Management Specification Version 4.1", AF-TM-0121.000, March 1999.

APPENDIX B GLOSSARY

AAA	Authentication, Authorization, and Accounting
AAL5	ATM Adaptation Layer 5
ADSL	Asymmetric Digital Subscriber Line
AF	Assured Forwarding
ANI	ASP to Network Interface
API	Application Program Interface
ARP	Address Resolution Protocol
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
ATMARP	ATM Address Resolution Protocol
ATMF	ATM Forum
ATU-C	Access Termination Unit - Central Office (at Access Network end)
ATU-R	Access Termination Unit - Remote (at customer end)
B-NT	Broadband Network Termination
BE	Best Effort
BGP	Border Gateway Protocol
BoD	Bandwidth on Demand
BRAS	Broadband Remote Access Server
CBR	Constant Bit Rate
CO	Central Office
COPS	Common Open Policy Service
CoS	Class of Service
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CSP	Corporate Service Provider
DHCP	Dynamic Host Configuration Protocol
Diffserv	Differentiate Services
DLC	Digital Loop Carrier
DNS	Domain Name Service
DS1	Digital Signal level 1 (1.544 Mbps)
DSCP	Differentiated Services (Diffserv) Code Point
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
EF	Expedited Forwarding
ESP	Encapsulating Security Payload
FQDN	Fully Qualified Domain Name
GFR	Guaranteed Frame Rate
iBGP	internal Border Gateway Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Secure Internet Protocol
ISP	Internet Service Provider
ITU-T	International Telecommunications Union - Technical
L2TP	Layer 2 Tunneling Protocol
L2TS	Layer 2 Tunnel Switch
L2oMPLS	Layer 2 over MPLS
LAC	Layer 2 Access Concentrator
LAN	Local Area Network
LD	Long Distance
LDAP	Lightweight Directory Access Protocol
LER	Label Edge Router

LLC	Logical Link Control
LSP	Label Switched Path
LNS	L2TP Network Server
MAC	Medium Access Control
MARS	Multicast Address Resolution Server
MASS	Multi-Application Selection Service
MBGP	Multicast Boarder Gateway Protocol
MPEG	Motion Pictures Expert Group
MPLS	Multi-Protocol Label Switching
MS/MD	Multi Session / Multi Destination Service
MTU	Message Transfer Unit
NAPT	Network Address Port Translation
NG-DLC	Next Generation Digital Loop Carrier
NHRP	Next Hop Resolution Protocol
NNI	Network to Network Interface
NSP	Network Service Provider
OC3	Optical Carrier 3
OSPF	Open Shortest Path First
PC	Personal Computer
PHB	Per Hop Behavior
PHY	Physical Layer
PNI	Premises to Network Interface
POP	Point of Presence
POS	Packet over SONET
PPP	Point-to-Point Protocol
PPPoA	Point-to-point Protocol over ATM
PPPoE	Point-to-Point Protocol over Ethernet
PTA	PPP Terminated Aggregation
PVC	Permanent Virtual Circuit
PVP	Permanent Virtual Path
QoS	Quality of Service
RADIUS	Remote Access Dial-In User Service
RAM	Remote Access Multiplexer
RFC	Request For Comments
RG	Routing Gateway
RSVP	ReSource reserVation Protocol
RT-DSLAM	Remote Digital Subscriber Line Access Multiplexer
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLO	Service Level Objective
SNAG	Service Network Architecture Group (DSL Forum)
SONET	Synchronous Optical Network
SVC	Switched Virtual Circuit
TCP	Transmission Control Protocol
TE	Traffic Engineering
TR	Technical Report (DSL Forum)
TV	Television
UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
UNI	User to Network Interface
VBR-nrt	Variable Bit Rate - non-Real Time
VBR-rt	Variable Bit Rate - Real Time
VC	Virtual Circuit
VCC	Virtual Circuit Connection
VLAN	Virtual Local Area Network
VoD	Video on Demand

VP	Virtual Path
VPC	Virtual Path Connection
VPN	Virtual Private Network
VoBB	Voice over Broadband
VoIP	Voice over Internet Protocol
WFQ	Weighted Fair Queuing

APPENDIX C PRODUCT AND SERVICES USE CASES

C.1 Subscriber Use Cases

This appendix includes some examples exploiting some aspects of the architecture. Please note some of these use cases will use real life examples of these services. Any specific service definitions are shown for example only and do not reflect a product definition by any of the contributors.

C.1.1 Bandwidth on Demand – the "Turbo" button

This specific scenario will describe a mechanism for dynamically increasing a subscriber's bandwidth. In this situation the subscriber, who has purchased service from a NSP that connects to the Regional Network via L2TP, is already connected with a specific destination or service and decides that they need additional bandwidth for a special function, such as a file download. Presently their DSL line is configured to shape downstream traffic at 768 Kbps. When they connected to their current Service Provider, they were provided with a series of tools to help manage the connection. These tools include the ability to display line statistics, including calculating average bandwidth utilization.

This application will also contain a button marked "Turbo Mode". Pressing this button will signal the network to change the subscriber's traffic shaping profile from its current rate to the next available tier. Specifically, new policy data is pushed to the BRAS for how to shape and rate limit that customers PPP session. For each press of the button, the subscriber can have their downstream traffic shaped to the next tier. In no case would the system permit the subscriber to select a speed tier where the low-end speed is faster than their DSL line is capable of sustaining.

The "Turbo" button could also be placed on a Service Provider's web page. Here it would, using a set of APIs provided by the Regional/Access Network, provide the necessary signaling back to the access equipment to reshape the subscriber's traffic as indicated and capture the necessary billing information.

C.1.2 Multi-Session/Multi-Destination Service (MS/MD)

Today's DSL subscriber is limited in the applications that they can select. They connect to a single Service Provider and have access only to those applications that this provider elects to provide. Currently, many of the popular applications are available over the public Internet. However, many corporations and universities have deployed firewalls that make access to these networks somewhat more cumbersome. The subscriber has to run Virtual Private Networking (VPN) software to attach to these firewalls and gain access. Some destinations are not available using VPN software either because they are so distributed to make VPNs impractical or there are concerns over using the public Internet for transport, no matter how secure the VPN software.

With MS/MD, the subscriber connects with PPPoE and logs in through the Access Network using a fully qualified domain name (FQDN). The PPP session is terminated at the BRAS, which performs a RADIUS proxy function for the destination/Service Provider. The domain portion of the name (the "ISP.NET" portion of Joe.User@ISP.NET) is used to select the Service Provider the subscriber wishes to connect to. The BRAS, prior to sending the RADIUS information, checks that customer's profile that contains a list of which locations or domains they are allowed to access. The username and password authentication is then used to grant access to the destination. Each destination or Service Provider is connected to the Regional/Access Network and traffic from the BRAS is routed and handed to the destination/Service Provider via IP.

In a similar fashion a second user within the premises, or the same user, may launch another session/application that is destine for yet another Service Provider. This session could be initiated via PPP as described above, or may use native IP over bridged Ethernet. The BRAS once again would relay authentication data, if the user profile allows, or may locally authenticate the user and route their session to its destination that is connected to the Regional/Access Network via an IP.

C.1.3 Bandwidth on Demand – Service based

With the MS/MD service above, it is now possible to contact multiple Service Providers. Some Application Service Providers, however, may require that, in order to deliver their service, the subscriber may need

more bandwidth than the DSL line is currently provisioned at. When the subscriber connects with these providers, their traffic shaping profile will be modified to support what the Service Provider specifies. In this case, the signaling necessary to perform this traffic shaping would be generated internally in the Access Network.

This use case would flow to the MS/MD case described above. There is one major addition to those scenarios, however. When the user is authenticated either directly by the BRAS, or by the proxy, the initiation of that session/application indicates that the specific bandwidth treatment for the authenticated user. Specifically, the RADIUS response that is received by the BRAS could also include profile information informing the BRAS how to shape that user's traffic.

This type of service could also be supported via an implicit "turbo" button. That is, a user, whose session is terminated (PPP or IP over bridged Ethernet) on the BRAS, starts an application at a specific Service Provider. The initiation of that application is analogous to the user pressing the turbo button and follows the turbo button use case described above. A major difference, however, is that rather than only being able to shape the aggregate PPP sessions the Service Provider collects, the specific application traffic flow within a PPP session is shaped.

C.2 Service Provider Use Cases

C.2.1 Quality of Service by Application Service Provider

Just like some services will require different traffic shaping, some applications may also be sensitive to delay and jitter. For these services, differentiated traffic delivery is available to Service Providers. Traffic from these Service Providers will be tagged in order to get preferred handling treatment within the Regional/Access Network. This means that, for example, IP video conferencing traffic would get preferred shaping and delivery over Internet traffic to the same subscriber. These types of services are only available to sessions that terminate (PPP or IP over bridged Ethernet) on the BRAS allowing the Regional/Access Network to have per flow IP awareness.

APPENDIX D SAMPLE MESSAGE EXCHANGE FOR BASIC SESSION ESTABLISHMENT WITH RSVP

This appendix includes an example message exchange establishing a dynamic QoS enabled service. This message exchange is not complete. Other logical elements or signaling protocols may be required. While certain protocols are explicitly shown, it should be used as a high level reference that will be updated in subsequent versions of the document.